Application of Rivada Networks LLC for Approval as a Spectrum Access System Administrator and an Environmental Sensing Capability Operator

GN Docket No. 15-319

TABLE OF CONTENTS

1.0 Introduction and Summary

Rivada Networks, LLC (Rivada) is pleased to submit this proposal to the Federal Communications Commission (FCC) to become a Spectrum Access System (SAS) Administrator and an Environmental Sensing Capability (ESC) Operator for the Citizens Broadband Radio Service (CBRS) as described in Title 47 of the Code of Federal Regulation Part 96 (47 CFR §96) in response to the FCC's Public Notices ("Wireless Telecommunications Bureau and Office of Engineering and Technology Establish Procedure and Deadline for Filing Spectrum Access System (SAS) Administrator(s) and Environmental Sensing Capability (ESC) Operator(s) Applications, GN Docket No. 15-319" and "Wireless Telecommunications Bureau and Office of Engineering and Technology establish 'Second Wave' Deadline for Proposals from Prospective Spectrum Access System (SAS) Administrator(s) and Environmental Sensing Capability (ESC) Operator(s); GN Docket no. 15-319").

Rivada's primary business is designing, integrating, building, and deploying fixed infrastructure and mobile communication systems and networks to support first responder personnel. Since Hurricane Katrina, Rivada has responded to almost every major disaster in the U.S., supporting multiple agencies including Department of Homeland Security (DHS), Department of Defense (DoD), Federal Emergency Management Agency (FEMA), the National Guard, the U.S. Army, and the U.S. Air Force. Rivada has deployed communication networks in over thirty states in the continental United States.

Since inception, Rivada's team has accumulated 97 patents worldwide for new technologies related to wireless communications and enhanced location services. Rivada has a further 200 patents pending globally. Dynamic Spectrum Arbitrage-Tiered Priority Access (DSATPA) is the world's first technology that seamlessly allocates excess cellular capacity to where it is most needed. Our capacity sharing technology is complementary to CBRS, allowing finer grained sharing of radio resources when used in combination.

Rivada has joined the Wireless Innovation Forum (WinnForum) Spectrum Sharing Committee (SSC), is in the process of joining the CBRS Alliance and will actively participate with the wireless industry to develop the standards, procedures and best practices required to maximize the value of the CBRS.

1.1 SAS/ESC Scope of Functions

The following section provides a detailed description of the functions that Rivada's Spectrum Assess System and Environment Sensing Capability will perform.

1.1.1 SAS Functionality

Rivada Networks, LLC (Rivada) will fully comply with 47 C.F.R §96 Subpart F - Spectrum Access System (SAS) and implement all the required functions of the SAS as described in Title 47 C.F.R §96.53, §96.55, §96.57, §96.59, §96.61, §96.63 and §96.66.

Rivada will comply with and fulfill the SAS purposes and functionality stated in 47 C.F.R §96.53, which include:

47 C.F.R §96.53 Spectrum access system purposes and functionality.
(a) To enact and enforce all policies and procedures developed by the SAS Administrator pursuant to §96.63.
(b) To determine and provide to CBSDs the permissible channels or frequencies at their location.
(c) To determine and provide to CBSDs the maximum permissible transmission power level at their

location.
(d) To register and authenticate the identification information and location of CBSDs.
(e) To retain information on, and enforce, Exclusion Zones and Protection Zones in accordance with §96.15 and §96.17.
(f) To communicate with the ESC to obtain information about federal Incumbent User transmissions and instruct CBSDs to move to another frequency range or cease transmissions.
(g) To ensure that CBSDs operate in geographic areas and within the maximum power levels required to protect federal Incumbent Users from harmful interference, consistent with the requirements of §96.15 and §96.21.
(h) To ensure that CBSDs protect non-federal Incumbent Users from harmful interference, consistent with the requirements of §96.17 and §96.21.
(i) To protect Priority Access Licensees from interference caused by other PALs and from General Authorized Access Users, including the calculation and enforcement of PAL Protection Areas, consistent with §96.25.
(j) To facilitate coordination between GAA users operating Category B CBSDs, consistent with §96.35.
(k) To resolve conflicting uses of the band while maintaining, as much as possible, a stable radio frequency environment.
(l) To ensure secure and reliable transmission of information between the SAS and CBSDs.
(m) To protect Grandfathered Wireless Broadband Licensees consistent with CFR 47 §90.1307 and CFR 47 §90.1338 and §96.21.
(n) To implement the terms of current and future international agreements as they relate to the Citizens Broadband Radio Service.
(o) To receive reports of interference and requests for additional protection from Incumbent Access users and promptly address interference issues.

1.1.1.1 SAS Information Gathering and Retention

Rivada's SAS will perform the function or meet the requirements detailed below:

47 C.F.R §96.55 Information gathering and retention.
(a) The SAS shall maintain current information on registered CBSDs, the geographic locations and configuration of protected FSS locations as set forth in §96.17, and the federal Incumbent User Exclusion Zones and Protection Zones.
(1) For registered CBSDs, such information shall include all information required by §96.39 and §96.45.
(2) SAS Administrators must make all information necessary to effectively coordinate operations between and among CBSDs available to other SAS Administrators.
(3) SAS Administrators must make CBSD registration information available to the general public, but they must obfuscate the identities of the licensees providing the information for any public disclosures.
(4) For non-federal Incumbent Users, the SAS shall maintain a record of the location of protected earth stations as well as the all registration information required by §96.17.
(b) The SAS shall maintain records not pertaining to federal Incumbent User transmissions for at least 60 months.
(c) The SAS shall only retain records of information or instructions received regarding federal Incumbent User transmissions from the ESC in accordance with information retention policies established as part of the ESC approval process.

(d) The SAS shall be technically capable of directly interfacing with any necessary FCC database containing information required for the proper operation of a SAS.
(e) The SAS shall process and retain acknowledgements by all entities registering CBSDs that they understand the risk of possible interference from federal Incumbent User radar operations in the band.

1.1.1.1 SAS Registration, Authentication, and Authorization of Citizens Broadband Radio Service Devices.

Rivada's SAS will perform the function or meet the requirements detailed below:

47 C.F.R §96.57 Registration, authentication, and authorization of Citizens Broadband Radio Service Devices.
(a) A SAS must register, authenticate, and authorize operations of CBSDs consistent with this part.
(b) CBSDs composed of a network of base and fixed stations may employ a subsystem for aggregating and communicating all required information exchanges between the SAS and CBSDs.
(c) A SAS must also verify that the FCC identifier (FCC ID) of any CBSD seeking access to its services is valid prior to authorizing it to begin providing service. A list of devices with valid FCC IDs and the FCC IDs of those devices is to be obtained from the Commission's Equipment Authorization System.
(d) A SAS must not authorize operation of CBSDs within Protection Zones except as set forth in §96.15.
(e) A SAS must calculate and enforce PAL Protection Areas consistent with §96.25 and such calculation and enforcement shall be consistent across all SASs.

1.1.1.2 SAS Frequency Assignment.

Rivada's SAS will perform the function or meet the requirements detailed below:

47 C.F.R §96.59 Frequency assignment.
(a) A SAS must determine the available and appropriate channels/frequencies for CBSDs at any given location using the information supplied by CBSDs, including location, the authorization status and operating parameters of other CBSDs in the surrounding area, information communicated by the ESC, other SASs, and such other information necessary to ensure effective operations of CBSDs consistent with this part. All such determinations and assignments shall be made in a non-discriminatory manner, consistent with this part.
(1) Upon request from the Commission or a CBSD, a SAS must confirm whether frequencies are available in a given geographic area.
(2) Upon request from the Commission, a SAS must confirm that CBSDs in a given geographic area and frequency band have been shut down or moved to another available frequency range in response to information received from the ESC.
(3) If a SAS provides a range of available frequencies or channels to a CBSD, it may require that CBSD to confirm which channel or range of frequencies it will utilize.
(b) Consistent with the requirements of §96.25, a SAS shall assign geographically contiguous PALs held by the same Priority Access Licensee to the same channels in each geographic area, where feasible. The SAS shall also assign multiple channels held by the same Priority Access Licensee to contiguous frequencies within the same License Area, where feasible.
(c) A SAS may temporarily assign PALs to different channels (within the frequency range authorized for Priority Access use) to protect Incumbent Access Users or if necessary to perform its required functions.

1.1.1.3 SAS Security.

Rivada's SAS will perform the function or meet the requirements detailed below:

47 C.F.R §96.61 Security.
(a) A SAS must employ protocols and procedures to ensure that all communications and interactions between the SAS and CBSDs are accurate and secure and that unauthorized parties cannot access or alter the SAS or the information it sends to a CBSD.
(b) Communications between CBSDs and a SAS, between an ESC and a SAS, between individual CBSDs, and between different SASs, must be secure to prevent corruption or unauthorized interception of data. A SAS must be protected from unauthorized data input or alteration of stored data.
(c) A SAS must verify that the FCC identification number supplied by a CBSD is for a certified device and must not provide service to an uncertified device.

1.1.1.4 SAS Administrators.

Rivada understands that the Federal Communications Commission will designate one or more SAS Administrators to provide nationwide service and that the FCC may, at its discretion, permit the functions of a SAS, such as a data repository, registration, and query services, to be divided among multiple entities; however, it shall designate one or more specific entities to be a SAS Administrator responsible for coordinating the overall functioning of a SAS and providing services to operators in the Citizens Broadband Radio Service. Rivada's SAS will perform the function or meet the requirements detailed below:

47 C.F.R §96.63 SAS Administrator.
(a) Maintain a regularly updated database that contains the information described in §96.55.
(b) Establish a process for acquiring and storing in the database necessary and appropriate information from the Commission's databases, including PAL assignments, and synchronizing the database with the current Commission databases at least once a day to include newly licensed facilities or any changes to licensed facilities.
(c) Establish and follow protocols and procedures to ensure compliance with the rules set forth in this part, including the SAS functions set forth in subpart F of this part.
(d) Establish and follow protocols and procedures sufficient to ensure that all communications and interactions between the SAS, ESC, and CBSDs are accurate and secure and that unauthorized parties cannot access or alter the SAS or the information transmitted from the SAS to CBSDs.
(e) Provide service for a five-year term. This term may be renewed at the Commission's discretion.
(f) Respond in a timely manner to verify, correct or remove, as appropriate, data in the event that the Commission or a party brings a claim of inaccuracies in the SAS to its attention. This requirement applies only to information that the Commission requires to be stored in the SAS.
(g) Securely transfer the information in the SAS, along with the IP addresses and URLs used to access the system, and a list of registered CBSDs, to another approved entity in the event it does not continue as the SAS Administrator at the end of its term. It may charge a reasonable price for such conveyance.
(h) Cooperate to develop a standardized process for coordinating operations with other SASs, avoiding any conflicting assignments, maximizing shared use of available frequencies, ensuring continuity of service to all registered CBSDs, and providing the data collected pursuant to §96.55.
(i) Coordinate with other SAS Administrators including, to the extent possible, sharing information, facilitating non-interfering use by CBSDs connected to other SASs, maximizing available General Authorized Access frequencies by assigning PALs to similar channels in the same geographic regions,

and other functions necessary to ensure that available spectrum is used efficiently consistent with this part.
(j) Provide a means to make non-federal non-proprietary information available to the public in a reasonably accessible fashion in conformity with the rules in this part.
(k) Ensure that the SAS shall be available at all times to immediately respond to requests from authorized Commission personnel for any and all information stored or retained by the SAS.
(l) Establish and follow protocols to respond to instructions from the President of the United States, or another designated Federal government entity, issued pursuant to 47 U.S.C. 606.
(m) Establish and follow protocols to comply with enforcement instructions from the Commission.
(n) Ensure that the SAS:
(1) Operates without any connectivity to any military or other sensitive federal database or system, except as otherwise required by this part; and
(2) Does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by this part to effectively operate the SAS.

1.1.1.5 SAS Responsibilities Related to Priority Access Spectrum Manager Leases.

Rivada's SAS will perform the function or meet the requirements detailed below:

47 C.F.R §96.66 SAS responsibilities related to priority access spectrum manager leases.
(a) A SAS Administrator that chooses to accept and support leasing notifications shall:
(1) Verify that the lessee is on the certification list, as established in §1.9046 of Title 47 of the CFR.
(2) Establish a process for acquiring and storing the lease notification information and synchronizing this information, including information about the expiration, extension, or termination of leasing arrangements, with the Commission databases at least once a day;
(3) Verify that the lease will not result in the lessee holding more than the 40 megahertz of Priority Access spectrum in a given License Area;
(4) Verify that the area to be leased is within the Priority Access Licensee's Service Area and outside of the Priority Access Licensee's PAL Protection Area; and
(5) Provide confirmation to licensee and lessee whether the notification has been received and verified.
(b) During the period of the lease and within the geographic area of a lease, SASs shall treat any CBSD operated by the lessee the same as a similarly situated CBSDs operated by the lessor for frequency assignment and interference mitigation purposes.

1.1.2 ESC Functionality

Rivada Networks, LLC (Rivada) will fully comply with 47 C.F.R §96 Subpart G – Environment Sensing Capability (ESC) and implement all the required functions of the SAS and the ESC as described in Title 47 C.F.R §96.67.

Specifically, Rivada understands that the primary purpose of the ESC is to facilitate coexistence of Citizens Broadband Radio Service users with federal and non-federal Incumbent Users through signal sensing. Rivada affirms that it is a non-government entity and will not rely on governmental agencies to affirmatively communicate information about the operations of incumbent radio systems except as allowed under 47 C.F.R. §96 Subpart G and that it will not operate without the approval of the Federal Communications Commission.

Rivada understands the provision that ESC equipment may be deployed in the vicinity of the Exclusion Zones and Protection Zones to accurately detect federal Incumbent User transmissions.

Rivada will fulfill the ESC requirements stated in 47 C.F.R §96.67(c), which include:

47 C.F.R §96.67(c) Environmental sensing capability Requirements
(1) Be managed and maintained by a non-governmental entity;
(2) Accurately detect the presence of a signal from a federal system in the 3550-3700 MHz band and adjacent frequencies using approved methodologies that ensure that any CBSDs operating pursuant to ESC will not cause harmful interference to federal Incumbent Users;
(3) Communicate information about the presence of a signal from a federal Incumbent User system to one or more approved SASs;
(4) Maintain security of detected and communicated signal information;
(5) Comply with all Commission rules and guidelines governing the construction, operation, and approval of ESCs;
(6) Ensure that the ESC shall be available at all times to immediately respond to requests from authorized Commission personnel for any information collected or communicated by the ESC; and
(7) Ensure that the ESC operates without any connectivity to any military or other sensitive federal database or system and does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by this part to effectively operate the ESC.

1.2 Key Personnel

The CBRS leadership team from Rivada provides a strong executive foundation with a team well versed in spectrum management; product development in the areas of high performance computing, algorithm development, and hardware design; as well as worldwide design, deployment, and operation of wireless networks.

Conor Allen: Conor is Senior VP and Head of Market Technology for Rivada. After beginning his career in the telecom sector, he spent many years meeting the demanding requirements of the financial services industry by developing solutions in high performance computing, application performance and tuning, and middleware agnostic APIs. As the former Global Head of R&D for NYSE Technologies, Conor formed advisory groups to foster closer relations with clients, while sitting on the NYSE Euronext Architecture Council to promote the use of common components and reduce product time to market. He is deeply experienced in evaluating new technologies and identifying technology partners. While at financial services firm, Cowen & Co., Conor built an option market making system from the ground up, again focusing on computational efficiency and speed.

John Meyer: John is VP of Technical Services for Rivada. He brings more than 30 years' experience in the mobile communications industry. Most recently, he implemented and tested Rivada's Dynamic Spectrum Arbitrage technology on a major infrastructure vendor's system. John's broad experience includes founding the U.S. operation of Mobile Systems International, an RF planning software and services company. He served as CTO and EVP of O2wireless when they purchased his RF Engineering services business. John also has decades of experience project managing domestic and international deployments of wireless networks. While at Comcast, John's responsibilities included evaluation of

WiFi, WiMAX and LTE performance opportunities. John began his career, spending 10 years with AT&T and Motorola as a software engineer.

David Sanders: David Sanders is an inventor, algorithm developer, hardware designer, and business founder. He serves as Rivada's Director of RF Technologies. David has worked in the wireless industry for more than 25 years, designing and deploying wireless networks throughout the world. He founded serval companies in the RF measurement sector, including Wider Networks, where he invented, developed and patented a receiver that identifies and processes signals below the noise floor, using novel techniques. He ran wireless network design and deployment companies that built networks in Germany, Italy and the US and well as a tower company in the telecom sector. Earlier in David's career, he played key role in development of Code Division Multiple Access (CDMA) network planning procedures for Qualcomm.

Peter Tenerelli: Peter Tenerelli provides expertise in spectrum management, software automation tools, process development, and training. He serves as Rivada's Director of Technology Adoption. Recently, Peter managed the demonstrations of Rivada's Dynamic Spectrum Arbitrage (DSA) technology to the Public Safety Communications Research (PSCR) lab and to many industry and government personnel. Earlier, he authored Sprint's Spectrum Planning Guidelines as part of the FCC's 800 MHz Rebanding initiative and developed the plan for an 800 MHz incumbent to migrate their equipment and 30,000 subscribers to a new band. Peter developed and implemented processes for the Dutch Federal Police that allow them to forecast their spectrum requirements. He also spent several years on the development of an airborne spectrum measurement system. Peter has spent more than 15 years working for leading vendors of automatic frequency planning tools and automatic cell planning tools, as well as ray-tracing propagation solutions. He has worked as an industry consultant and instructor teaching about wireless telecom.

Please see section 1.3.2 for information about our corporate leadership.

1.3 Rivada Networks LLC Business Structure

1.3.1 Corporate Overview

This section provides the qualifications of Rivada Networks.

Rivada Networks is a privately held company that is focused on unlocking the potential of spectrum sharing, capacity sharing and shared networks. The company holds an array of patents for its signature technology, Dynamic Spectrum Arbitrage, which allows bandwidth on a commercial network to be traded and allocated in real time. Rivada views the CBRS initiative as complimentary and aligned with its focus on cellular capacity sharing.

Rivada's primary business is designing, integrating, building, and deploying fixed infrastructure and mobile communication systems and networks to support first responder personnel. Since Hurricane Katrina, Rivada has responded to almost every major disaster in the U.S., supporting multiple agencies including Department of Homeland Security (DHS), Department of Defense (DoD), Federal Emergency Management Agency (FEMA), the National Guard, the U.S. Army, and the U.S. Air Force. Rivada has deployed communication networks in over 30 states in the continental United States.

The firm maintains a structured organization that remains nimble and responsive to the changing landscape of technological innovation. Rivada Networks is working under NAICS 517210 Wireless Telecommunications Carriers, which is defined as "under 1,500 employees and providing services cellular phone services, paging services, wireless Internet access, and wireless video service." The firm is also listed under eight additional NAICS codes. Rivada maintains a staff primarily composed of engineers, program/project managers, and technical subject matter experts – all experienced experts in their discipline. Rivada has supported numerous military and government organizations to quickly mobilize and deploy multiple task forces simultaneously during both natural and man-made disasters, as well as National Special Security Events. Rivada has supported various DoD and DHS agencies over the last eleven years, and was instrumental in helping US Northern Command (USNORTHCOM) develop USNORTHCOM Publication 6-02, Deployable Communication Standards.

Rivada's continuous leadership and evolution in the networking space uniquely positions us to perform, meet, and exceed the requirements and expectations for a SAS Administrator.

Rivada has designed over 150 different Government tactical LMR and cellular systems that have been deployed over 225 times in response to natural disasters: Hurricanes Ike, Gustav, Katrina and Rita; tornados in Missouri, Kansas, and Georgia; wildfires in Texas and California; National Special Security Events; and exercise and training events like Ardent Sentry, Vigilant Shield, and National Level Exercise 2011. Our team has a thorough understanding of the unique and critical requirements of public safety tactical communications, including the deployment and operation of communication systems and networks.

Rivada possesses a wealth of radio communications system experience, including: tower infrastructure; microwave backhaul; land mobile radio (LMR); frequency coordination; site permitting; quality audits; site integration coordination; and end user equipment. Since 2004, Rivada has supported the government on over 20 projects and has amassed a solid history of project management experience on communications systems and other larger projects. Rivada possesses knowledge and experience working with legacy systems and equipment; as technology has matured and evolved, our know-how and skill sets have evolved and grown. Rivada continues to be on the leading edge of technological breakthroughs, as evidenced by our development of Dynamic Spectrum Arbitrage-Tiered Priority Access (DSATPA).

DSATPA is the world's first technology that seamlessly allocates excess cellular capacity to where it is most needed. DSATPA is a patented cellular capacity optimization and sharing technology that will be used by Public Safety and commercial wireless operators to provide access to cellular capacity where and when it is needed most. DSATPA is complementary to CBRS, ultimately allowing finer grained sharing of radio resources when used in combination.

1.3.2 Corporate Leadership

1.3.2.1 Board of Directors

Declan Ganley: Declan Ganley is an entrepreneur, founder, chairman and Co-CEO of Rivada Networks, a leading provider of open access wireless networks and public safety broadband communications services to a broad range of government customers. Rivada Networks pioneered the development of its patented Dynamic Spectrum Arbitrage-Tiered Priority Access technology.

Michael P. Jackson: Michael Jackson served as Deputy Secretary of the Department of Homeland Security from 2005 until 2007. In this role, Mr. Jackson served as Department of Homeland Security's chief operating officer, with responsibility for managing the day-to-day operations.

Richard B. Myers: General Myers became the fifteenth Chairman of the Joint Chiefs of Staff on Oct. 1, 2001. In this capacity, he served as the principal military advisor to the President, the Secretary of Defense, and the National Security Council.

Peter Goldscheider: Peter has 25 years' experience as a senior executive in finance. Before jointly establishing EPIC, he was Vice President for Marketing and Sales and Member of the Board of Zürich Kosmos Insurance Company in Austria. He began his professional career with IBM Austria.

George Foresman: George was confirmed by the United States Senate in December 2005 as America's first Under Secretary of Preparedness at the Department of Homeland Security. On March 31, 2007, he became the first Under Secretary for National Protection and Programs at DHS.

Admiral James Loy: Admiral Loy completed a 45-year career in public service in 2005, retiring as the first Deputy Secretary of Homeland Security, a position that he held from 2003 to 2005. In this capacity, he was involved in all aspects of consolidating 22 separate agencies into one unified cabinet department as well as managing the day-to-day activities of the agency.

Field Marshal the Lord Guthrie: Charles Guthrie was Chief of the Defense Staff in the United Kingdom between 1997 and 2001 and Chief of the General Staff of the British Army between 1994 and 1997. He is a member of the House of Lords. He was created a life peer after retiring as Chief of the Defense Staff.

Don De Marino: Don is an international businessman and former government official. He served as Deputy Assistant Secretary of Commerce and as Director of the U.S.-Saudi Joint Economic Commission. He is presently Chairman of the National U.S.-Arab Chamber of Commerce.

Gabriela Lippe-Holst: Gabriela co-founded Acqupart and Acqufin, two international investment management companies, and currently serves as the Chairperson of the Board at Acqupart and CEO of Acqufin. Prior to this, Gabriela spent nearly 15 years at Swiss Re between Zurich and New York where, as a Managing Director, she held legal and risk management responsibilities that extended to Latin America.

Gov. Jeb Bush: Governor Bush was the 43rd governor of the state of Florida, serving from 1999 through 2007. Prior to and after his tenure as Governor, Bush was actively involved in the private sector helping to build the largest full service real estate company in South Florida and owning and operating successful consulting and investing businesses.

Gov. Martin O'Malley: Governor O'Malley served two terms as Governor of Maryland from 2007-2015. Prior to that, he served two terms as Mayor of Baltimore. He co-chaired the National Governors Association's Task Force on Homeland Security and was the first Maryland governor to deliver interoperable radio communications for all of Maryland's first responders.

1.3.2.2 Key Corporate Leadership

JOSEPH J. EUTENEUER: CO-CEO and CFO, Americas

Prior to joining Rivada Joe served as Chief Financial Officer of Sprint Corporation from April 2011 until December 2015. He has more than 30 years of experience in the Telecommunications sector, focusing on financial, operational, and planning processes' improvement. He is a senior executive and board member with a track record of accomplishment in Fortune 50 and large public company environments.

Over the course of his distinguished career in telecom and media, Euteneuer has held CFO and EVP positions at Sprint, Qwest Communications (now CenturyLink), XM Satellite Radio, now Sirius XM Satellite Radio, and Comcast. Joe is a CPA and holds an MBA from Duke and an undergraduate degree from ASU. He has been with Rivada Networks since 2016.

JOSEPH SANZO: CHIEF NETWORK OFFICER

Joe is Chief Network Officer with Rivada Networks, and has more than 26 years of professional experience in telecommunications consulting, design, engineering, development and operations. He has led the deployment and operation of major wireless networks in North America, Europe, Middle East, Asia and Australia.

CLINT SMITH: CHIEF SCIENTIST/TECHNOLOGY OFFICER

Clint has more than 20 years of experience in all aspects related to fixed and wireless telecommunications including system design, project management, budgeting, operations, sales and management. He is an internationally known technical author whose books and industry trade articles are used extensively in the telecommunication industry. Clint is the lead inventor of our organization and has many years of wireless industry and technology experience.

PETER CAMPBELL: CHIEF INFORMATION OFFICER

Prior to joining Rivada, Peter was CIO with Sprint Corp. In his CIO capacity, he managed OSS/BSS Application Development and Maintenance, Data Center Operation, Cybersecurity and IT Services for a National Network service provider. His 35-year management experience includes network engineering, construction, provisioning, maintenance, regulatory matters, labor relations, customer service and finance. He has significant experience in major project planning and delivery, successful vendor management, outsourcing and contract negotiations and IT transformation.

KAREN FREITAG: CHIEF CUSTOMER OFFICER

Karen Freitag is an executive leader with experience in sales, marketing and operations. For more than 25 years, Karen has successfully built high performing sales teams in the telecommunications sector. Her prior experience comes from IBM, Nortel Networks, Ericsson and most recently as President, Enterprise Solutions at Sprint. Karen has received numerous industry awards and was most recently named to the "Influential Women of Wireless" list compiled by wireless industry publication FierceWireless in September 2015, and was a 2014 finalist for Capacity Magazine's Executive of the Year Award for Industry Contribution.

KEN FIELDS: CHIEF NETWORK MONETIZATION OFFICER

Mr. Fields has more than 30 years of experience as an investment manager and risk manager on Wall Street and as a hedge-fund manager, most recently at Natron Group where he served as the Chief Investment Officer. Having focused throughout his career on Global-Macro investing, Mr. Fields has in-

depth experience in most global markets with significant expertise in derivatives and a strong focus on illiquid and emerging markets. Mr. Fields has been a frequent participant in new markets and was integrally involved in the design and rollout of the "US Dollar-Index" future which is a trade-weighted currency basket that remains an important trading / hedging tool today.

For information about key personnel on the project, please see Section 1.2.

1.3.3 Financial Capability

Rivada has sufficient funds, support from its investors and access to capital to support the engineering, development, testing, certification and operation of our proposed SAS and ESC for the minimum five-year term contemplated by the Commission's Part 96.63(e) rule following approval as an Administrator.

Rivada has invested heavily in multiple R&D programs since inception and continues to do so. This project is complimentary to Rivada vision of shared capacity networks and making much more efficient use of valuable and scarce spectrum resources, and as such is a priority project for Rivada.

1.3.4 Fee Structure

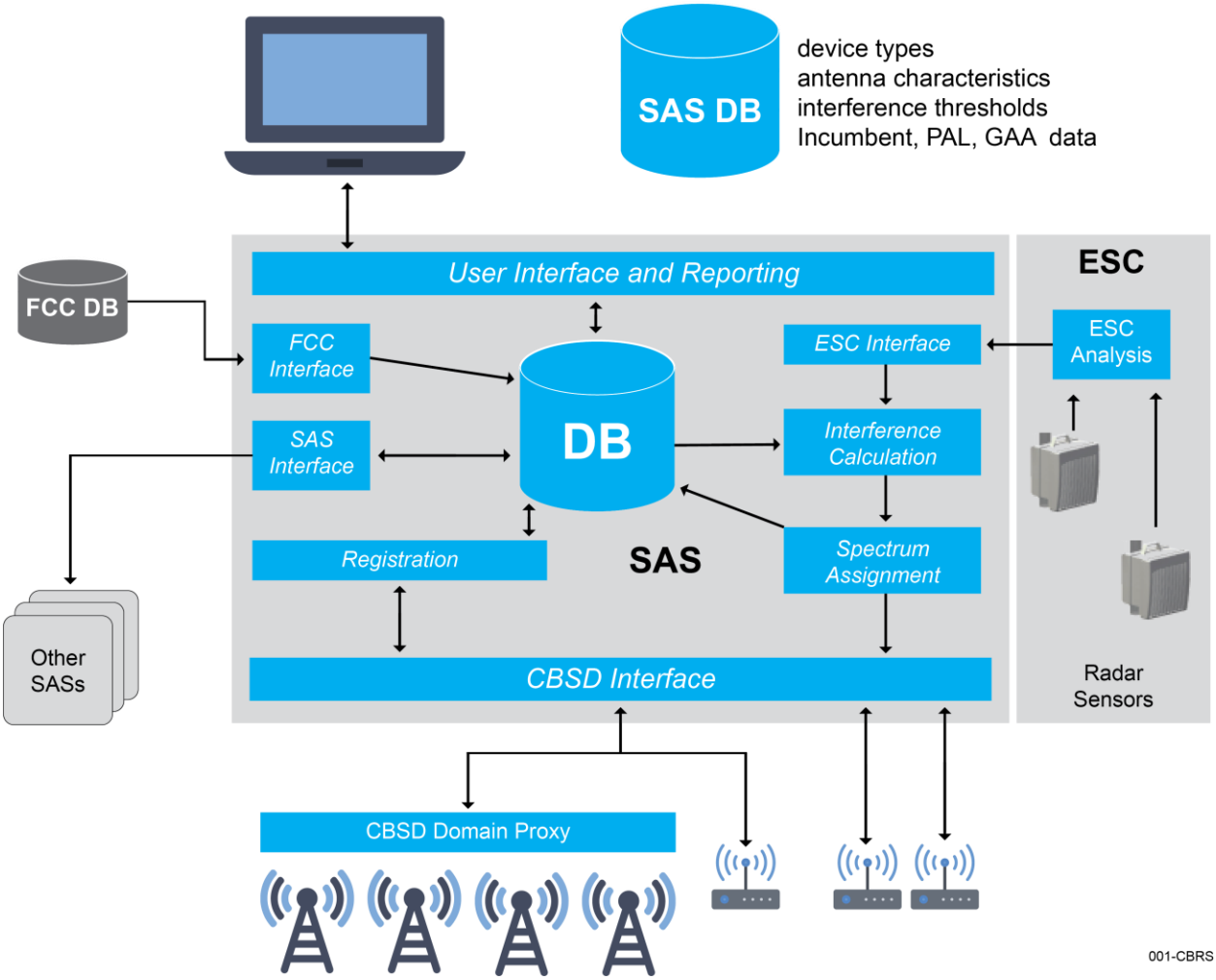
Consistent with the Commission's goal of encouraging the rapid development of 3.5 GHz devices and services, Rivada Networks will charge users reasonable and competitive fees. If requested, Rivada Networks will work with the Commission to review its fees and modify such fees if they are found to be unreasonable by the Commission.

1.4 SAS to ESC Communications

The Rivada SAS to Rivada ESC interface is proprietary and is not currently subject to standardization. The Rivada SAS to ESC interface will be generally consistent with the CBRS Communications Security Technical Specification (CBRS COMSEC TSWINNF-15-S-0065-V2.0.0). If WInnForum produces a standard SAS to ESC protocol, Rivada will consider adopting the standard, as we recognize the benefits of standard interfaces.

Rivada expects the communication to be near real-time and well within the timing required by the standard expected to allow a SAS to evacuate CBRS users from spectrum if an incumbent user is detected.

1.5 SAS and ESC Architecture



1.5.1 Registration

Confirming and verifying the identity of any CBSD seeking to use the 3.5 GHz Band prior to authorizing its operation consistent with §96.57 of the Commission's rules, including preventing CBSD operations within any Protection Zones and calculating and enforcing Priority Access License (PAL) Protection Areas, using a combination of:

- Rules and Policy Engines
- Interference Estimations
- Frequency Assignments per given geographical areas and
- Verification against the FCC databases of approved and licensed CBSDs.

1.5.2 Interference Calculation

The interference calculation module will estimate the power that would be received at each incumbent and PAL device from all PAL and GAA devices in the network database. This calculation is performed for each new registration. The potential interference is calculated from the sum of the received powers of all devices.

1.5.3 Spectrum Assignment

If the result of the interference calculation shows harmful interference to an incumbent or PAL device, the SAS has multiple options for mitigation. These include reducing output powers of devices, restricting the use entirely of a device, and forcing frequency changes. Rivada will follow the recommendations of the WInnForum SSC.

1.5.4 Interface and Reporting

The interface and reporting function provides a means for government and SAS personnel to have visibility into CBRS spectrum usage. It will provide the following information.

- Reports and audits of the current databases;
- Non-compliance reports for any CBSD's frequency assignment that has not followed the frequency allocation requests of the SAS;
- Activity logs of SAS and SAS to CBSD interactions;
- Spectrum/channel availability per census tract; and CBSD statuses connected to the SAS and presence of incumbent activity in the census tracts.

1.5.5 Domain Proxy Server

The domain proxy server provides a standard way for CBSDs to communicate securely with the SAS. The Rivada SAS will support the interfaces developed by the WInnForum.

1.6 Propagation Model

Rivada will use two different propagation modelling approaches, based on the calculation type.

To calculate interference to FSS incumbents, a point-to-point model is more suitable, such as those used to calculate attenuation along microwave paths. On the other hand, a point-to-multipoint model is more sensible when calculating coverage areas (Protection Areas, etc.) or interference to these areas.

Scenario	Propagation Model Type
GAA or PAL interference to FSS	Point-to-point
GAA or PAL interference to areas such as protection areas	Point-to-multipoint

We recognize the potential benefits of standardizing propagation modelling techniques across multiple SAS administrators. We are willing to consider different methods than those described here, based on recommendations from the FCC, WInnForum, or other parties.

Point to Point Model

Rivada will use a point to point model that relies on the physical geometry of the propagation path between the transceivers, such as models used to calculate attenuation along microwave paths. The model accounts for distance from the transmitter, antenna gains on the propagation path, attenuation due to clutter, diffraction by obstacles, among others. Digital databases to support these kinds of calculations are readily available.

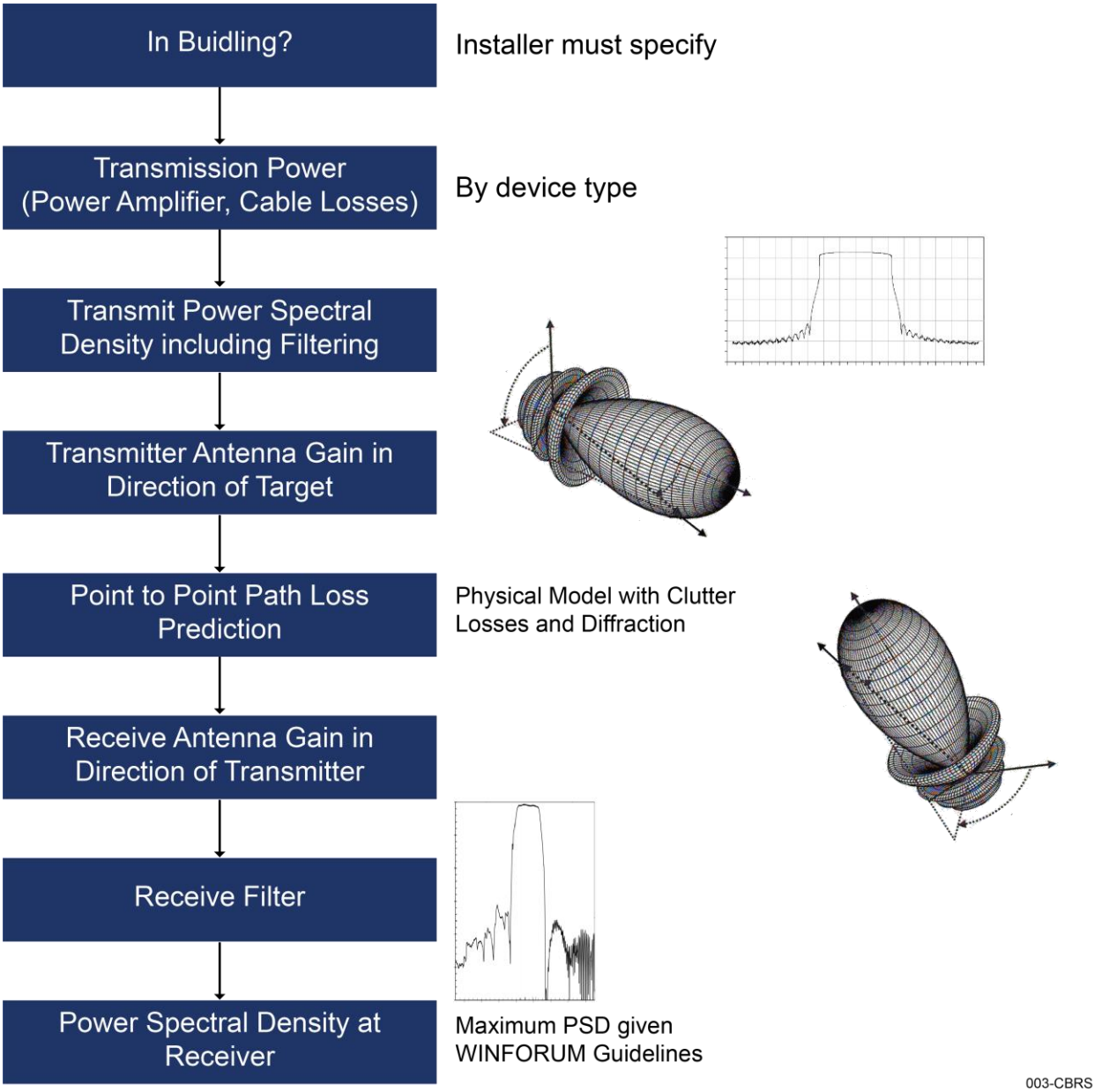
Point to Multipoint Model

Rivada agrees that there are benefits to SAS Administrators standardizing on the same propagation model. At the same time, we recognize that an empirical model (e.g. Hata family of models) can be

manifested as many models, simply by changing the coefficients of the model's equation. Therefore, any standardization should include methods for choosing the values selected for propagation model coefficients or other input variables. Rivada will consider the industry consensus when making a final choice of point to multipoint propagation model.

Power Spectral Density Calculation Steps

To calculate the interfering power spectral density (PSD), other factors beyond the propagation model must be considered. The PSD interference calculation will consider filtering and other factors of the entire link. The figure below illustrates these factors.



1.7 Software Security and Lifecycle

Rivada will provide methods for keeping software and firmware updated to the latest versions. This will entail an automated system that will be developed to conform with the best practice being developed by the WInnForum. At present, we expect that over-the-air programming will be employed. Whenever possible, updates will be performed during the maintenance window to avoid any possibility of SAS downtime.

Rivada will continually monitor security and perform periodic testing to insure detection of any vulnerability in the system. In addition, security alerts and other information will be provided to the operators to keep them informed.

The following describes, at a high level, the Rivada Secure Operations Center (SOC):

The Security Operations Center (SOC) ensures that the network is protected against cyber-attacks and maintaining security elements of confidentiality (protection of information), integrity (trustworthiness of the information passed around in the network), and availability (preventing bad actors from blocking access to legitimate network users.)

The SOC ensures proper operation and monitoring of firewalls and intrusion prevention systems. The SOC also performs an “internal affairs” function: security information and event management (SIEM) to ensure that internal personnel are not causing a security breach. Finally, the SOC analyzes the “access logs” for security threats and inappropriate patterns of behavior. These logs are the history showing which internal personnel performed which actions on which components and what time.

An example of a SOC responsibility is an investigation and resolution of suspicious patterns of access attempts to the system.

1.8 SAS Administrator and ESC Operator Affirmation (47 C.F.R §96)

Rivada Networks, LLC (Rivada) hereby affirms that it and its SAS and ESC will comply with all the applicable rules in addition to all the applicable enforcement mechanisms and procedures related to being a SAS Administrator and an ESC Operator.

2.0 SAS Specific Requirements

2.1 Data Retention

Rivada's SAS will comply with the data retention requirements of 47 C.F.R. § 96.55. The SAS will maintain a database of the information required to implement Part 96 requirements. For CBSDs, the database will include the following:

1. Location - automatic or certified professional installer supplied
2. RF parameters
3. Certified professional installer identification
4. Device operator information
5. Authorization type
6. Individual device information
    a. FCC ID
    b. manufacturer's serial number
7. Grant status

Rivada will make all information necessary to effectively coordinate operations between and among CBSDs available to other SAS Administrators.

Rivada SAS will maintain a record of the location of protected earth stations and Wireless Internet Service Providers, who have priority until 2020, as well as the all registration information required by Section 96.17 of the FCC's rules.

2.1.1 Data Security

All Rivada SAS interfaces will use Transport Layer Security (TLS), a protocol that provides privacy and data integrity between two communicating applications. TLC will assure the following:

- Secure, confidential, and tamper-proof communications between the SAS, CBSDs, ESC, sensors, external databases, Federal users and other SAS operations.
- That CBSD devices are valid users of the SAS, that only inputs from approved ESC sensors are recognized, and that SAS-to-SAS synchronization is performed only with certified SAS operators.

Rivada will adopt the CBSD information management, registration procedures and interface protocols requirements from WInnForum specifications, including the SAS to SAS Interface (WINNF-16-P-0003) and the SAS to CBSD Interface (WINNF-15-P-0062) and any subsequent revisions.

2.1.2 Data Verification

Rivada's SAS will verify that the CBSD's FCC Identification and Call Sign match the corresponding entry in the FCC databases.

Rivada's SAS will compare the entered address of the CBSD to the entered coordinates to verify that they agree. We will also verify that all locations reside within the geographic operational area of our SAS.

Rivada will authenticate devices using the certificates issued to device manufacturers.

Rivada will provide user accounts to FCC personnel who need access to the Rivada SAS. These users will be verified with two-factor user authentication.

2.2 Interference Protection

The Rivada SAS will resolve various sources of interference between and among Citizens Broadband Radio Service users and/or Incumbent users to protect them from harmful interference per the rules.

The Rivada SAS will ensure that federal incumbent users do not receive harmful interference per the Commission's rules.

For CBSDs operating in the 3550 – 3650 MHz band, as described in the Commission's rules within §96.15(a):

- The Rivada SAS will ensure that CBSDs and End User Devices do not cause harmful interference to and accept interference from federal Incumbent Users authorized to operate in the 3550-3700 MHz band and below 3550 MHz
- The Rivada SAS will only authorize the use of CBSDs consistent with information on federal frequency use obtained from an approved ESC, except as provided in this section.
- For Category A CBSDs, the Rivada SAS will maintain Exclusion Zones maintained along the Coastline, as shown at *ntia.doc.gov/category/3550-3650-mhz*. The Rivada SAS will also maintain Exclusion Zones around federal radiolocation sites as set forth at *ntia.doc.gov/category/3550-3650-mhz*. The Rivada SAS will update exclusion zones based on updates to the list of protected federal radiolocation sites by the Commission and NTIA. Rivada SAS will maintain and enforce Exclusion Zones until one or more ESCs are approved and used by at least one SAS, in accordance with §96.67. Thereafter, Exclusion Zones shall be converted to Protection Zones and treated as such by the Rivada SAS.
    - The Rivada SAS, once approved, may authorize Category A CBSDs in geographic Areas outside of Exclusion Zones before an ESC is approved.
    - Once an ESC is approved and used by at least one SAS, the Rivada SAS will authorize only Category A CBSDs consistent with information on federal frequency use provided to the Rivada SAS by an approved ESC.
    - The Rivada SAS will authorize only Category B CBSDs consistent with information on the presence of a signal from a federal system provided to the Rivada SAS by an approved ESC.
- Within 300 seconds after the ESC communicates that it has detected a signal from a federal system in a given area, or the Rivada SAS is otherwise notified of current federal incumbent use of the band, the Rivada SAS will either confirm suspension of the CBSD's operation or its relocation to another unoccupied frequency, if available. If the President of the United States (or another designated Federal Government entity) issues instructions to discontinue use of CBSDs pursuant to 47 U.S.C. 606, the Rivada SAS will instruct CBSDs to cease operations as soon as technically possible.
- The Rivada SAS will comply with additions to or modifications of Exclusion Zones or Protection Zones issued by the Commission to protect current and future federal Incumbent Users.
- The Rivada SAS will comply with the Commission's instructions that may temporarily extend or modify Exclusion Zones and Protection Zones to protect temporary operations by federal Incumbent Users.

For CBSDs operating in the 3650 – 3700 MHz band as described in the Commission's rules within §96.15(b):

- The Rivada SAS will ensure that CBSDs and End User Devices do not cause harmful interference to and will accept interference from federal Incumbent Users authorized to operate in the 3500-3700 MHz band.
- The Rivada SAS shall maintain Exclusion Zones for an 80km radius around the federal radiolocation sites listed in 47 CFR 90.1331 and 47 CFR 2.106, US 109. The Rivada SAS will enforce these Exclusion Zones until one or more ESCs are approved and used by at least one SAS, in accordance with §96.67. Thereafter, the Rivada SAS will provide interference protection based on Protection Zones.
- The Rivada SAS will authorize CBSDs within these Protection Zones consistent with information on the presence of a signal from a federal system provided to the SAS by an approved ESC, in accordance with §96.67.
- Within 300 seconds after the ESC communicates that it has detected a signal from a federal system in a specific area, or the Rivada SAS is otherwise notified of current federal incumbent use of the band, the Rivada SAS will either confirm suspension of the CBSD's operation or its relocation to another unoccupied frequency. If the President of the United States (or another designated Federal Government entity) issues instructions to discontinue use of CBSDs pursuant to 47 U.S.C. 606, the Rivada SAS will instruct CBSDs to cease operations as soon as technically possible.

2.3 Incumbent User Interference Protection

The Rivada SAS will ensure that non-federal FSS earth stations and grandfathered 3650-3700 MHz licensees are protected from harmful interference consistent with the Commission's rules.

For protection of existing fixed satellite service (FSS) earth stations in the 3600-3700 MHz Band and 3700-4200 MHz Band as described in the Commission's rules within §96.17:

For FSS earth stations licensed to operate in the 3600-3700 MHz band

- The Rivada SAS will regularly update its list of FSS earth stations licensed to operate in the 3600-3700 MHz band listed at *www.fcc.gov/cbrs-protected-fss-sites* and provide protection consistent with shall be protected from CBSD operation consistent with §96.17.
- The Rivada SAS will confirm that the conditions set forth in §96.21(c) are satisfied to provide protection to FSS earth stations in the 3650-3700 MHz band
- The Rivada SAS will use the Co-channel and Blocking criteria to determine if the FSS earth stations licensed to operate in the 3600-3700 MHz band are receiving harmful interference. These criteria are found in the Commission's rules in §96.17(a)(2) and §96.17(a)(3).

For FSS earth stations licensed to operate in the 3700-4200 MHz band

- The Rivada SAS will regularly update its list of FSS earth stations licensed to operate in the 3700-4200 MHz band and entitled to protection from CSBD operation. The source for this list is www.fcc.gov/cbrs-protected-fss-sites.
- The Rivada SAS will protect licensed FSS earth stations used for satellite telemetry, tracking, and control (TT&C) operations as per the Commission's rules in §96.17(b). For licensed 3700-4200 MHz earth stations not used for TT&C operations, the Rivada SAS will apply the rules of §96.17(f).

- The Rivada SAS will use the Out-of-Band Emissions into FSS and Blocking criteria to determine if the FSS earth stations licensed to operate in the 3600-3700 MHz band are receiving harmful interference. These criteria are found in the Commission's rules in §96.17(b)(1) and §96.17(b)(2).

For CBSDs operating within areas that may cause interference to FSS earth stations

Per the Commission's rules in §96.17(e): Should the licensee of the FSS earth station and the authorized user of the CBSD mutually agree that said CBSDs may operate within areas that may cause interference to FSS earth stations in excess of the levels described in §96.17(a) and (b), the Rivada SAS Administrator shall consider whether the Rivada SAS will enforce the terms. If the Rivada SAS then agrees to enforce the terms, it will promptly communicate the agreement to all other SAS Administrators.

For FSS earth station licensees in the 3600-3700 and 3700-4200 MHz bands who request additional protection to prevent harmful interference

Per the Commission's rules in §96.17(f): The Rivada SAS will establish a process to receive and address such requests, consistent with §96.53(o) and 96.63 and will make good faith efforts to address interference concerns, consistent with Rivada's other responsibilities under this part. In addressing such requests, the Rivada SAS shall assume that 3700-4200 MHz earth stations are utilizing filters with the characteristics described in §96.17(a)(3) or (b)(2) as appropriate for the 3600-3700 or 3700-4200 MHz band.

For operation near the Canadian and Mexican borders as described in the Commission's rules within §96.19:

- The Rivada SAS will implement the terms of current and future international agreements with Mexico and Canada about Citizens Broadband Radio Service operation in the 3550-3700 MHz band.

For protection of existing operators in the 3650-3700 MHz Band as described in the Commission's rules within §96.21:

- The Rivada SAS will consider Grandfathered Wireless Broadband Licensees to have been granted Incumbent User status consistent with 47 CFR §90.1307 and 47 CFR §90.1338. Notwithstanding this status, Grandfathered Wireless Broadband Licensees shall not cause harmful interference to federal Incumbent Users and grandfathered FSS earth stations consistent with the rules governing Citizens Broadband Radio Service operators in this part.
    - The Rivada SAS will provide Incumbent User protections for a Grandfathered Wireless Broadband Licensee only within its Grandfathered Wireless Protection Zone.
    - The Rivada SAS will apply Incumbent User protections for a Grandfathered Wireless Broadband Licensee only for the conditions cited in the Commission's rules in §96.21(a)(2). If the Grandfathered Wireless protection zones or applicable frequency ranges are modified by the Commission, the Rivada SAS will enforce the modified rules.
- The Rivada SAS will provide a mechanism for registration of the Grandfathered Wireless Protection Zones.

- The Rivada SAS will protect Grandfathered Wireless Protection Zones and operational frequencies consistent with the technical rules in part 90, subpart Z, consistent with the transition period set forth in 47 CFR §90.1307 and 47 CFR §90.1338.
- The Rivada SAS will protect authorized grandfathered FSS earth stations in the 3650-3700 MHz band, consistent with the existing protection criteria in 47 CFR part 90, subpart Z, until the last Grandfathered Wireless Broadband Licensee's license expires within the protection area defined for a particular, grandfathered, FSS earth station. Thereafter, the Rivada SAS will apply protection criteria in §96.17 applicable to FSS earth stations in the 3600-3700 MHz band.

2.4 SAS-SAS Communication

Rivada will implement the WInnForum SAS-SAS protocol (SAS-SAS Protocol Technical Specification WINNF-16-S-0096-V1.0.0) and will support ongoing revisions as they are approved. The specification provides a communications and security specification, mandating mutual authentication and minimum encryption levels and cipher suites. Records are exchanged between SAS peers via HTTPS POST (Push Type) and HTTPS GET (Pull Type) requests encoded as JSON messages to allow synchronization of state between peer SASs. SAS-SAS Protocol exchange entities include:

- SAS Administrators
- SAS Implementations
- CBSD Types
- CBSDs
- Incumbents
- ESC Sensors
- Zones
- Coordination Events

Rivada expects that synchronization between SASs will be near real-time.

2.5 SAS Functions

Rivada, as an approved SAS Administrator, will be performing all SAS functions.

2.6 SAS Ecosystem Interfaces and Protocols

The following section describes the interfaces and protocols that will be used by elements of the CBRS ecosystem, CBSDs, SASs, ESCs to communicate with each other.

2.6.1 SAS-CBSD Communication

The Rivada SAS will implement the standardized the WInnForum SAS-CBSD protocol specification (SAS-CBSD TS WINNF-16-S-0016-V1.0.1) and will support the interface pursuant to any subsequent revisions.

This protocol, using JSON encoded messages over HTTPS POST, provides for the following request reply message exchanges that control the lifecycle of operation of a CBSD:

- Registration
- Spectrum Inquiry
- Spectrum Grant Request
- Heartbeat
- Spectrum Grant Relinquishment

The heartbeat message, as detailed in the specification, will ensure that CBSDs will only operate when connected to and authorized by an approved SAS.

The details of messages and the procedures are described in detail in the specification.

2.6.2 SAS-SAS Communication

The Rivada SAS will implement standardized the WInnForum SAS-CBSD protocol specification (SAS-SAS Protocol Technical Specification WINNF-16-S-0096-V1.0.0) and will support the interface pursuant to any subsequent revisions.

The specification provides a communications and security specification, mandating mutual authentication and minimum encryption levels and cipher suites. Records are exchanged between SAS peers via HTTPS POST (Push Type) and HTTPS GET (Pull Type) requests encoded as JSON messages to allow synchronization of state between peer SASs. SAS-SAS Protocol exchange entities include:

- SAS Administrators
- SAS Implementations
- CBSD Types
- CBSDs
- Incumbents
- ESC Sensors
- Zones
- Coordination Events

Rivada expects that synchronization between SASs will be near real-time.

2.6.3 SAS-ESC Communications

As previously stated in Section 1.4, the communication protocol between Rivada's SAS and ESC will be proprietary, however it will generally be consistent with the WInnForum CBRS Communications Security Technical Specification (CBRS COMSEC TSWINNF-15-S-0065-V2.0.0). If an industry consensus standard interface emerges, Rivada will consider implementing such a standard. Additionally, Rivada will implement the proprietary interface to any FCC approved third-party ESC should it be necessary.

2.7 Data Retention

Rivada affirms that it will abide by Section 96.55 of the Commission's rules and will only retain records and information or instructions received regarding federal transmissions from the ESC in accordance with information retention policies established as part of the ESC approval process.

2.8 Security

Rivada will implement the security requirements of the SAS and ESC to comply with the security requirements of 47 CFR §96 in the following manner:

- The Rivada Security Operations Center (SOC) shall provide security services to ensure that unauthorized parties cannot access or alter the SAS or otherwise corrupt the operation of the SAS in performing its intended functions, consistent with the Commission's rules:
    - The Security Operations Center (SOC) ensures that the SAS/ESC/sensor network is protected against cyber-attacks and maintaining security elements of confidentiality

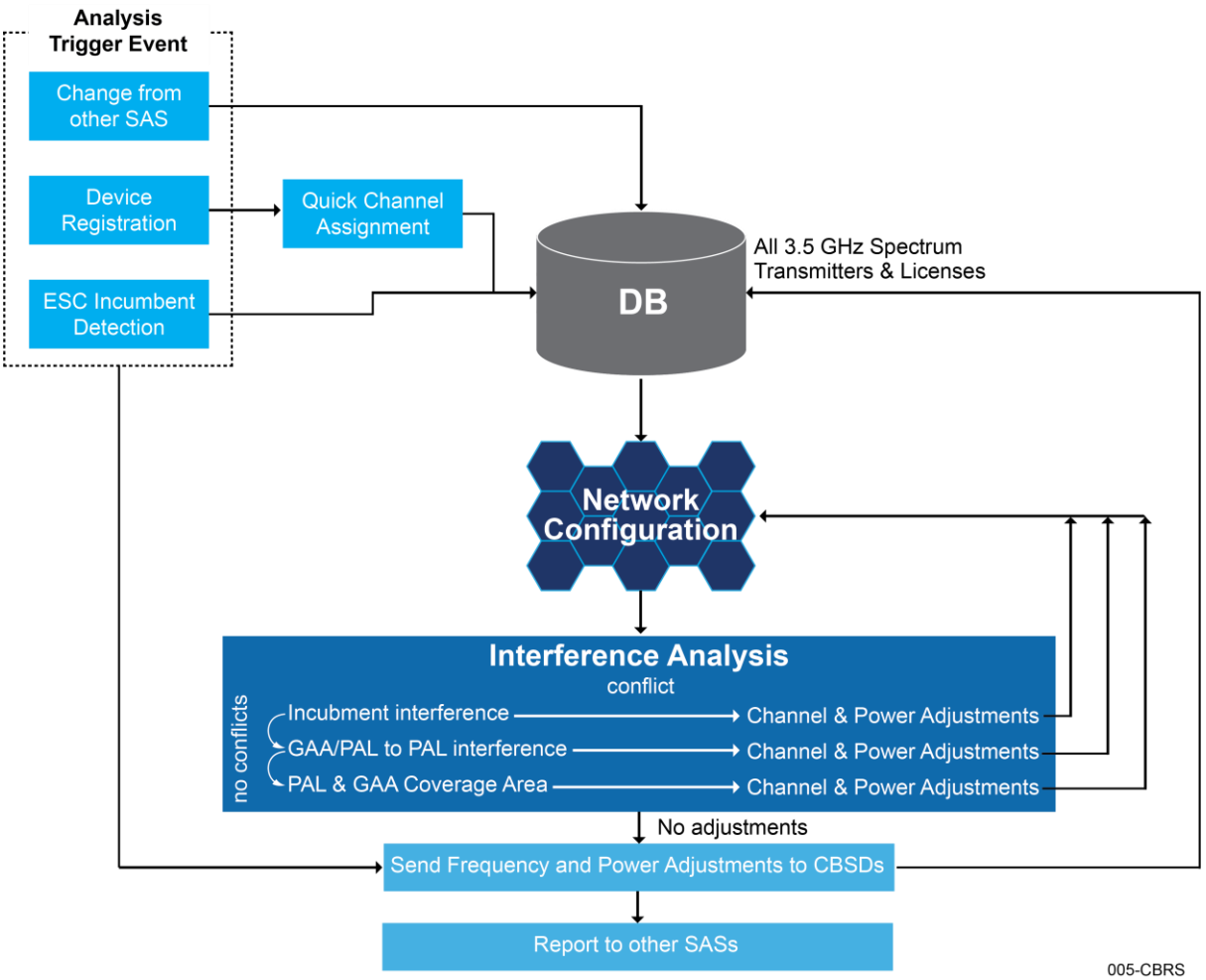
(protection of information), integrity (trustworthiness of the information passed around in the network), and availability (preventing bad actors from blocking access to legitimate network users.)
    - The SOC ensures proper operation and monitoring of firewalls and intrusion prevention systems. The SOC also performs an "internal affairs" function: security information and event management (SIEM) to ensure that internal personnel are not causing a security breach. Finally, the SOC analyzes the "access logs" for security threats and inappropriate patterns of behavior. These logs are the history showing which internal personnel performed which actions on which components and what time.
    - An example of a SOC responsibility is an investigation and resolution of suspicious patterns of access attempts to the system.

- All Rivada SAS interfaces will use the latest version of Transport Layer Security (TLS), a protocol that provides privacy and data integrity between two communicating applications. Currently, that is version 1.2. TLS will assure the following:
    - Secure, confidential, and tamper-resistant communications between the SAS, CBSDs, ESC, sensors, external databases, Federal users and other SAS operations.
    - That CBSD devices are valid users of the SAS, that only inputs from approved ESC sensors are recognized, and that SAS-to-SAS synchronization is performed only with certified SAS operators. Rivada will adopt the CBSD information management, registration procedures and interface protocols requirements from WInnForum specifications, including the SAS to SAS Interface (WINNF-16-P-0003) and the SAS to CBSD Interface (WINNF-15-P-0062).
- The Rivada SAS to ESC interface will be generally consistent with the CBRS Communications Security Technical Specification (CBRS COMSEC TSWINNF-15-S-0065-V2.0.0). In the event that WInnForum produces a standard SAS to ESC protocol, Rivada will consider adopting the standard, as we recognize the benefits of standard interfaces.
- Further, Rivada will adopt the CBSD information management, registration procedures and interface protocols requirements from WInnForum specifications, including the SAS to SAS Interface (WINNF-16-P-0003) and the SAS to CBSD Interface (WINNF-15-P-0062).
- Rivada's SAS will verify that the CBSD's FCC Identification and Call Sign match the corresponding entry in the FCC databases. Rivada's SAS will compare the entered address of the CBSD to the entered coordinates to verify that they agree. We will also verify that all locations reside within the geographic operational area of our SAS. The Rivada SAS will refuse service to CBSDs whose FCC ID cannot be verified.
- Rivada will authenticate devices using the certificates issued to device manufacturers.
- Rivada will provide user accounts to FCC personnel who need access to the Rivada SAS. These users will be verified with two-factor user authentication.
- For SAS-to-SAS communications, Rivada will implement the WInnForum SAS-SAS protocol (SAS-SAS Protocol Technical Specification WINNF-16-S-0096-V1.0.0) and will support ongoing revisions as that are approved. The specification provides both communications and security specifications, mandating mutual authentication and minimum encryption levels and cipher suites. Records are exchanged between SAS peers via HTTPS POST (Push Type) and HTTPS GET (Pull Type) requests encoded as JSON messages to allow synchronization of state between peer SASs.
- For SAS to CBSD communications, the Rivada SAS will implement standardized the WInnForum SAS-CBSD protocol specification (SAS-CBSD TS WINNF-16-S-0016-V1.0.1) and will support the

interface pursuant to any subsequent revisions. This secure protocol, using JSON encoded messages over HTTPS POST, provides for request reply message exchanges that control the lifecycle of operation of a CBSD.

- The Rivada SAS will employ different levels of user access based on the user's need to know the various types of information.
- The Rivada SAS will encrypt its stored data that will protect sensitive information such as incumbent operational activity, among others.
- The Rivada SAS will obfuscate the identities of the licensees when making CBSD registration information available to the general public.

2.9 Dynamic Workflows



The chart above shows the workflow Rivada will take to control PAL and GAA power levels and channel assignments. There are three trigger events that require a new interference analysis.

1. Update from another SAS
2. A Response from the ESC with New Incumbent Information
3. A Registration from a GAA or PAL Device

The interference analysis and corresponding channel assignment and power control is a complex problem with each decision potentially affecting other interference calculations. Therefore, whenever a trigger event occurs, the entire interference analysis must be rerun. The database in the figure above represents the current configuration of all GAA, PAL and incumbent devices, along with their operating parameters. The interference analysis algorithm will be run on the entire system.

Use Case: Adjacent Blocking

The adjacent blocking requirements protect the FSS front end from excessive total power in the entire range of the filter. CBSDs on any channel will add to the adjacent blocking power and must be accounted for. This analysis will use the transmit and receive spectrum characteristics as shown in section 1.6 Propagation Model.

Use Case: Out-of-Band Emissions

The FCC has created an out of band emission limit of -13 dBm/MHz for devices. This value will be assumed for the out of band power contribution to an incumbent user.

Use Case: Aggregate Co-channel

Rivada will calculate the sum of the contributions of interference from every GAA and PAL device within proposed ranges of an incumbent user.

2.10 FCC Authorized Access

Rivada will provide 24/7 secure web based access for authorized commission personnel as required by FCC's Part 96 rules. This interface will offer several levels of access for both reading and modifying data as required. Access can also be limited based on specific areas or locations. Various users will establish sign-on credentials appropriate to their authorization levels. Rivada will validate the users' authorization level with the appropriate Point of Contact at the Commission. Alternative communications (email for example) methods will also be provided.

Various reports will also be available to FCC personnel on either an on demand or periodic basis.

3.0 ESC Specific Requirements

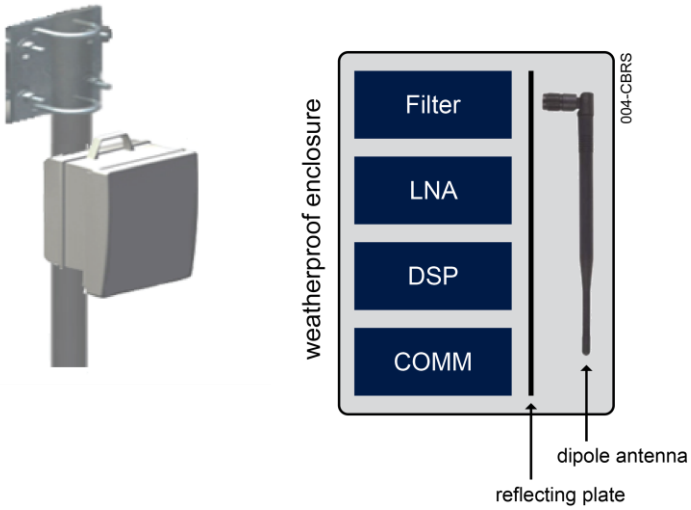
3.1 SAS-ESC Communications

As previously stated in Section 1.4, the communication protocol between Rivada's SAS and ESC will be proprietary. It will however be generally consistent with the WInnForum CBRS Communications Security Technical Specification (CBRS COMSEC TSWINNF-15-S-0065-V2.0.0) (ComSec). If an industry consensus standard interface emerges, Rivada will consider implementing such a standard. The ComSec specification provides for mutual authentication, forward security and advanced encryption standards, ensuring that unauthorized parties cannot access or alter the ESC, or otherwise corrupt the operation of the ESC in performing its intended functions.

The ESC will communicate with the SAS using JSON encoded messages over HTTPS POST. At a high level, the ESC will provide the minimum information required for the SAS to protect incumbent users from harmful interference from CBRS users. Additionally, the ESC will send heartbeat messages to the SAS to indicate the continued correct functioning of the ESC and its sensor network.

3.2 Type of Sensors

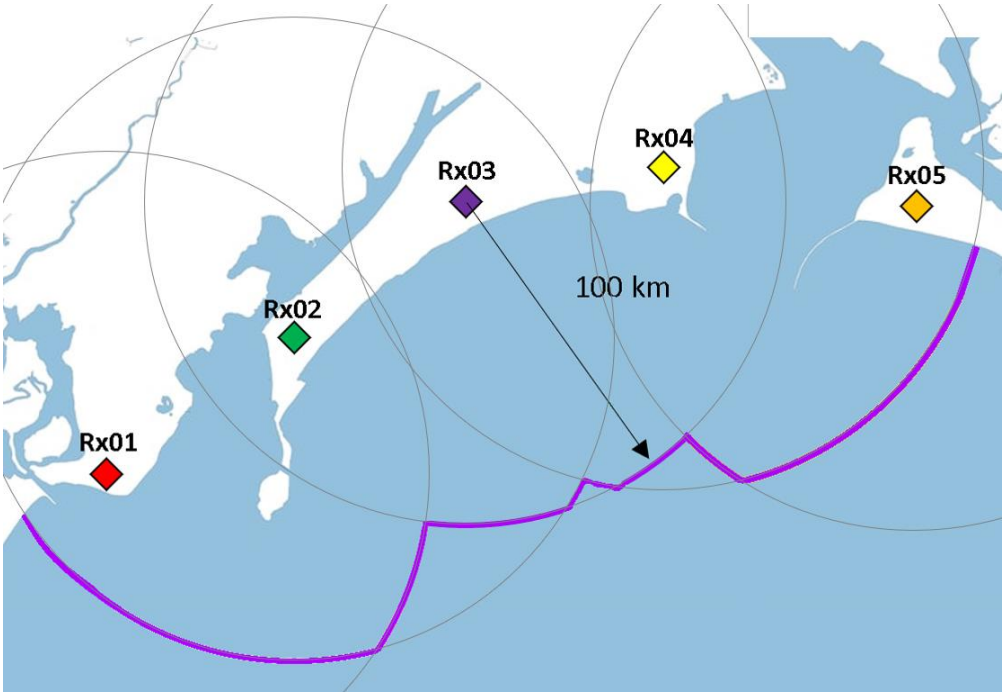
Rivada will build a sensor out of commercially available parts or complete RF receiver systems.



There are many options available. The sensor will have communications capability as well, through commercial wireless networks and WiFi.

3.2.1 Sensing Architecture

Rivada believes that reasonably accurate detection of naval radar requires the inputs from at least two sensors. Each sensor will have a detection radius of about 100 kilometers along the coast, depending, most importantly, on the height above sea level of the sensor to mitigate the loss due to Earth's curvature.



With these constraints and as illustrated in the figure above, Rivada has determined that a proper spacing of sensors is less than 75 km along the coast.

3.2.2 Sensing Thresholds

Rivada will follow the WInnForum guidelines for sensing thresholds. Rivada believes that the sensing threshold should be the minimum power spectral density that has a reasonable likelihood of being a ship radar. False positives can be removed by processing at the ESC. An individual sensor must analyze the received signal in frequency and time to determine whether that signal was likely to be from a ship's radar. The main characteristics of the radar signal are listed below. These will be used to determine whether a radar signal was received or not.

- Characteristic Value
- Pulse repetition rate 1 kHz
- Pulse width 0.9 µs
- Antenna rotation period 4 s

In the frequency domain, the detection algorithm would look for a proper frequency and bandwidth. In the time domain, the sensor would analyze the pulse spacing. Initially, signals that meet the criteria of exceeding the noise floor by a reasonable margin, e.g. 21 dB, and meet the time and frequency characteristics of the radar systems would be reported to the ESC. For a 1 MHz bandwidth and 3 dB noise figure, the noise level is about -111 dBm. Assuming a signal to noise requirement of 21 dB, the detection threshold would be -90 dBm. Over time, the techniques for detecting radar signals and the appropriate thresholds will be refined.

3.2.3 Processing of Sensor Data

If the sensor's detection algorithm determines that a radar signal has been received, the sensor will send back the power level of the detection and the frequency characteristics. Given the messages received at

the ESC from a collection of sensors, the ESC will make the decision about whether radar is present and from where it could be emanating. For a radar to be present, the same signal must be detectable in a large area at approximately the same time.

3.2.4 Sensor Sensitivity

Rivada expects the sensor to have a noise figure of 7 dB or less. This should easily achievable with commercially available products. For a 1 MHz bandwidth, this corresponds to a sensitivity of -104 dBm.

3.2.5 Sensor Resiliency to Receiver Front-End Saturation and Burn-Out

The sensor will have a dynamic range exceeding 65 dB, so saturation will occur with received signals greater than -39 dBm, using the values assumed in Section 3.2.4, above. The sensor will report saturation events to the ESC. The receiver will not burn out with received powers lower than 0 dBm.

3.2.6 Safeguards for Operational Information

Rivada will put in place safeguards to ensure that the ESC does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals the locations or movements of any federal system.

3.3 ESC to Sensor Interface

Rivada will embed a wireless communications module into the sensor. The interface between the sensors and Rivada's ESC will be proprietary. The ESC will maintain regular communication with the sensors to confirm that the sensors are operating. If a sensor is not responding, the ESC will report to the SAS. The SAS will then restrict the use of incumbent frequencies in the coverage area of that sensor. If the SAS loses communications with the ESC, all frequencies within the protected zone will be restricted.

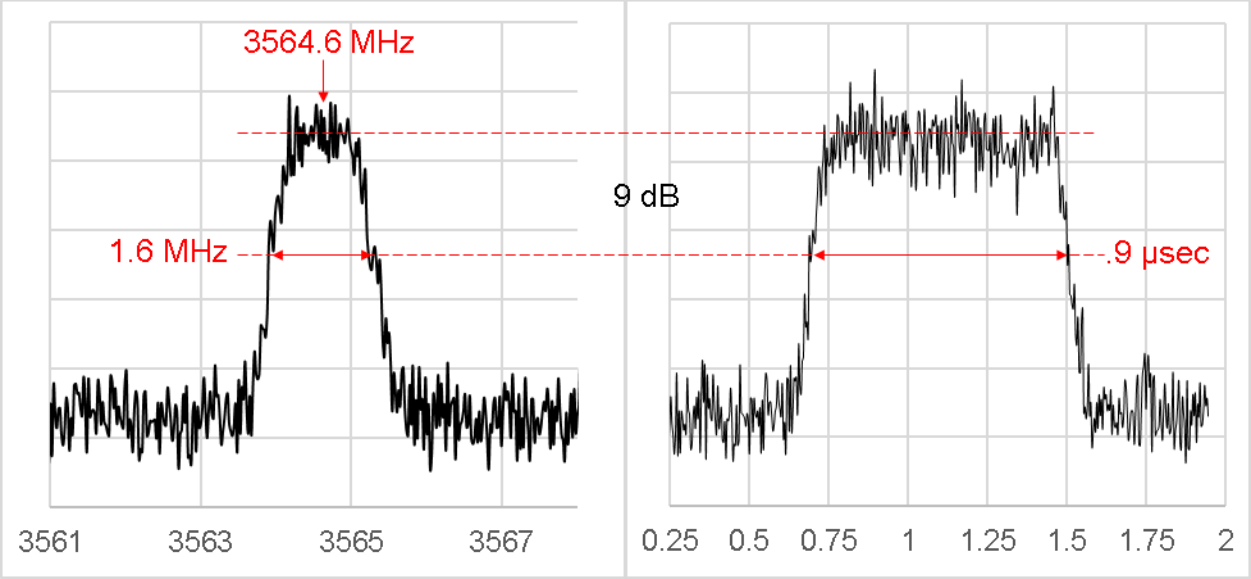
Each ESC will have a unique hardware ID and a GPS receiver. All data packets returned to the ESC will contain the following

- unique hardware ID
- latitude and longitude
- time stamp

When the detection threshold is exceeded, the packet will also contain the following information.

- frequency of the detected signal
- 9 dB bandwidth of the signal
- The 9 dB burst length
- power of the signal.

These values are illustrated in the figure below.



To maintain the highest level of security, Rivada plans to send no other information back to the ESC. All the information sent will use standard security and encryption protocols.

The Rivada Security Operations Center (SOC) shall provide security services to ensure that unauthorized parties cannot access or alter the ESC or individual sensors or otherwise corrupt the operation of the ESC in performing its intended functions:

- The Rivada Security Operations Center (SOC) ensures that the SAS/ESC/sensor network is protected against cyber-attacks and maintaining security elements of confidentiality (protection of information), integrity (trustworthiness of the information passed around in the network), and availability (preventing bad actors from blocking access to legitimate network users.)
- The SOC ensures proper operation and monitoring of firewalls and intrusion prevention systems. The SOC also performs an "internal affairs" function: security information and event management (SIEM) to ensure that internal personnel are not causing a security breach. Finally, the SOC analyzes the "access logs" for security threats and inappropriate patterns of behavior. These logs are the history showing which internal personnel performed which actions on which components and what time.
- An example of a SOC responsibility is an investigation and resolution of suspicious patterns of access attempts to the system.

All Rivada ESC interfaces will use the latest version of Transport Layer Security (TLS), a protocol that provides privacy and data integrity between two communicating applications. Currently, that is version 1.2. TLS will assure the following:

- Secure, confidential, and tamper-resistant communications between the SAS, CBSDs, ESC, sensors, external databases, Federal users and other SAS operations.
- That CBSD devices are valid users of the SAS, that only inputs from approved ESC sensors are recognized, and that SAS-to-SAS synchronization is performed only with certified SAS operators. Rivada will adopt the CBSD information management, registration procedures and interface

protocols requirements from WInnForum specifications, including the SAS to SAS Interface (WINNF-16-P-0003) and the SAS to CBSD Interface (WINNF-15-P-0062).

The Rivada SAS to ESC interface will be generally consistent with the CBRS Communications Security Technical Specification (CBRS COMSEC TSWINNF-15-S-0065-V2.0.0). In the event that WInnForum produces a standard SAS to ESC protocol, Rivada will consider adopting the standard, as we recognize the benefits of standard interfaces.

For further information on Rivada's security procedures, please see section 2.8

4.0 Cross Reference Table

	FCC Requirements	Rivada Section
1	A detailed description of the scope of the functions that the SAS and/or ESC would perform.	1.1
2	A demonstration that the prospective SAS Administrator or ESC operator possesses sufficient technical expertise to operate a SAS and/or ESC, including the qualifications of key personnel who will be responsible for operating and maintaining the SAS and/or ESC.	1.2
3	The prospective SAS Administrator or ESC operator must demonstrate that it is financially capable of operating a SAS and/or ESC for a five year term. The proposal must include a description of the prospective SAS Administrator or ESC operator's business structure including ownership information. To the extent that the proponent will rely on fees to support its operations, the proposal should also describe the fee collection process and the entities from which the fees will be collected.	1.3
4	A description of how data will be securely communicated between the SAS and its associated ESC and how quickly and reliably these communications will be accomplished.	1.4
5	Technical diagrams showing the architecture of the SAS and/or ESC and a detailed description of how each function operates and how each function interacts with the other functions.	1.5
6	A description of the propagation model and any other assumptions that the prospective SAS Administrator or ESC operator proposes to use to model operations and facilitate coordination in the band.	1.6
7	A description of the methods that will be used to update software and firmware and to expeditiously identify and address security vulnerabilities.	1.7
8	An affirmation that the prospective SAS Administrator and/or ESC operator (and its respective SAS and/or ESC) will comply with all the applicable rules as well as applicable enforcement mechanisms and procedures.	1.8

	SAS Proposal must also provide the following:	
1	A detailed description of how the SAS will retain, secure, and verify information from CBSDs (including location data), licensees, associated ESCs, and other SASs.	2.1
2	A demonstration that the SAS will can resolve various sources of interference between and among Citizens Broadband Radio Service users and/or Incumbent users	2.2
3	A description of how the SAS will ensure that non-federal FSS earth stations and grandfathered 3650-3700 MHz licensees are protected from harmful interference consistent with the rules.	2.3
4	A description of how coordination will be effectuated (e.g., through data synchronization) between multiple SASs, if multiple SASs are authorized, and how quickly this synchronization of data will be accomplished.	2.4
5	If the prospective SAS Administrator will not be performing all SAS functions, it must provide information on the entities operating other functions and the relationship between itself and these other entities. In particular, it must address how the Commission can ensure that all of the requirements for SAS Administrators in Part 96, subpart F are satisfied when SAS functions are divided among multiple entities, including a description of how data will be transferred among these various related entities and SASs, if multiple SASs are authorized, and the expected schedule of such data transfers (i.e., real-time, once an hour, etc.).	2.5
6	A description of the methods (e.g., interfaces, protocols) that will be used by: (1) CBSDs to communicate with the SAS; (2) the SAS to communicate with CBSDs; (3) the SAS to communicate with other SASs; and, if applicable, (4) the SAS to communicate with one or more ESCs. The prospective SAS Administrator must also describe the procedures, if any, which it plans to use to verify that a CBSD can properly communicate with the SAS.	2.6
7	An affirmation that, consistent with section 96.55 of the Commission's rules, the SAS will only retain records and information or instructions received regarding federal transmissions from the ESC in accordance with information retention policies established as part of the ESC approval process.	2.7

	SAS Proposal must also provide the following:	
8	A description of the security methods that the prospective SAS Administrator plans to use to ensure that unauthorized parties cannot access or alter the SAS or otherwise corrupt the operation of the SAS in performing its intended functions, consistent with the Commission's rules	2.8
9	Descriptions of dynamic use-case scenarios for how the SAS will manage and assign spectrum resources to ensure that geographically and spectrally adjacent operations are coordinated consistent with the Commission's rules. Use case scenarios should include the methodology and protection approach for cases of radio interference due to adjacent blocking, out-of-band emissions, and aggregate co-channel interference. Describe how multiple SASs will coordinate the calculation of aggregate interference for protecting Incumbent users and Priority Access licensees.	2.9
10	A description of the methods that the SAS will use to make information stored or retained by the SAS available in response to a request from authorized Commission personnel.	2.10

	ESC Proposal must also include:	
1	A description of the methods (e.g. interfaces, protocols) that will be used by the ESC to communicate with the SAS. It must include a description of the security methods or protocols that will be used to ensure that unauthorized parties cannon access or alter the ESC or otherwise corrupt the operation of the ESC in performing its intended functions.	3.1
2	A description of the sensing methodology it will use to detect federal transmissions and determine that the spectrum needs to be evacuated. This description must include a detailed description of the type of sensors to be used (i.e., infrastructure or device based), the sensing architecture to be employed, the sensing thresholds, any processing of sensor data, sensor sensitivity, and sensor resiliency to receiver frontend saturation and burn-out. The prospective ESC operator must also provide a description of the safeguards that will be used to "ensure that the ESC does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required to effectively operate the ESC by Part 96."	3.2

	ESC Proposal must also include:	
3	A description of the methods (e.g., interfaces, protocols) that will be used by sensors to communicate with the ESC and the procedures, if any, that it plans to use to verify that all sensors can communicate with the ESC in a timely and secure manner. It must include a description of the security methods or protocols that will be used to ensure that unauthorized parties cannot access or alter the ESC or individual sensors or otherwise corrupt the operation of the ESC in performing its intended functions.	3.3